



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/327,477	06/08/1999	YASUTSUGU KURODA	826.1547/JDH	5479

21171 7590 09/09/2003

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER

NOBAHAR, ABDULHAKIM

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 09/09/2003

9

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/327,477

Applicant(s)

KURODA ET AL.

Examiner

Abdulahkim Nobahar

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-10, 12-19 and 22-26 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-10, 12-19 and 22-26 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on ____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) ____.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-5, 8-9, 17 and 22-26 are rejected under 35 U.S.C. 102(b) as being anticipated by Boebert et al (5,502,766) (hereinafter Boebert).

Regarding claims 1, 3, 8-9, 17 and 22-23, Boebert discloses a data communication system for the secure storage, transfer and sharing of data in a local/wide area network of computers (see, for example, abstract, column 5, lines 39-46 and Fig. 3). Each computer system has a fixed or removable media for storing data and a crypto media controller corresponding to the recited encryption unit (see, for example, Fig. 5). The data stored in the media is encrypted/decrypted with a media key corresponding to the recited individual key (see, for example, Fig. 6b, Fig. 14, column 5, lines 59-67 and column 10, lines 1-5). The media key is assigned to in each computer system's media when it is initialized (i.e., before the use of media). An enclave key that corresponds to the recited common key is provided for each organization (group) for encryption of data that is transmitted from one point to another in the network (see, for example, Figs. 16, 21 and 24, column 5, lines 48-58, column 9, lines 64-67 and column 14, lines 57-61). A key management crypto (located in the security server of the

organization) that corresponds to the recited main electronic data storage of each group, generates the media key (individual key) for and distributes it to each computer system (see, for example, Fig. 16 and column 13, lines 43-51).

Regarding claims 2 and 4-5, Boebert discloses that a key management unit located on secure computer (corresponding to the recited main electronic data storage) provides the cryptographic keys including the enclave key (group key) (see, for example, column 5, lines 1-4 and column 9, lines 22-32). The enclave key is distributed to each computer system by the key management unit to be used for encryption of transmitting data (see, for example, column 11, lines 52-57 and column 25, lines 48-58).

Regarding claims 24-26, these claims are rejected as applied to the like elements of claims 1 and 22-23 as stated above and further the following:

Boebert discloses a data communication system for a local and a wide (global) area network of computers that storage media in each computer is assigned with a media UID and each device (computer) has its own attributes that defines the security attributes of that device (see, for example, column 10, lines 43-67 and column 28, lines 51-60).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 6-7, 10, 12-16 and 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boebert et al (5,502,766) (hereinafter Boebert) in view of Mittra (5,748,736).

Regarding claim 6, Boebert does not expressly disclose a computer system (an electronic data storage) as a management apparatus to manage the main electronic apparatuses in the network (group). Mittra, however, teaches a hierarchical level system in which a main group security controller (GSC) manages the security of the entire system as well as other trusted intermediary (TI) servers that correspond to the recited main electronic data storage apparatuses (see, for example, column 4, lines 5-20, column 7, lines 28-39, column 12, line 67 and Fig. 1). Each TI serves a sub-group and provides the encryption keys to each one of its sub-group members (see, for example, column 6, line 62-column 7, line 14). The Mittra's hierarchical structure also verifies members in the process of group communication (see, for example, column 4, lines 11-19 and column 11, lines 8-14). The GSC provides an encryption key (corresponding to the individual key) and the group key to the TIs in the system (see, for example, column 8, lines 23-31 and column 10, lines 36-42).

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time the invention was made, to provide a management apparatus to manage the main devices of each group as taught in Mittra in the system of Boebert, because it would provide a high level of security for the group and effectively managing the changes occur in the group (column 3, lines 15-17 and column 3, lines 43-50).

Regarding claim 7, Mittra teaches that a public cryptosystem can be used for encrypting messages to be transmitted across the network (see, for example, column 9, lines 54-61).

Regarding claim 10, Mittra teaches the use of a key corresponding to the recited master key, by all members in the group separate from the group key (see, for example, column 12, lines 5-15).

Regarding claim 12, this claim is rejected as applied to the like elements of claims 2 and 4 as stated above and further the following:

Boebert discloses that in generation of keys, inputted data by an authorized individual, data from a table or any other combination of data may be used (see, for example, column 13, lines 43-51).

Regarding claims 13 and 14, these claims are rejected as applied to the like elements of claims 2 and 4 as stated above and further the following:

Mittra teaches a hierarchical structure of groups consist of members in which each group is managed by an intermediary trusted (TI) server (see, for example, column 4, lines 20-25 and column 7, lines 1-14).

Regarding claims 15, 16, 18 and 19, Boebert does not expressly disclose the use of a hierarchical structure to manage the groups of the electronic data storage apparatuses in a higher and lower levels fashion and the group key to be dependent upon a hierarchical level of group. Mittra, however, teaches the use of a hierarchical order for the groups (see, for example, column 12, lines 30-60, and Fig. 1) to manage the groups and the group keys. In Mittra's system as shown in Fig. 1 there is a member (TI) at a group with a higher level that controls and manages the lower level group(s). The communication (transmission of data) from a member at the higher level group to a member at a lower level group is done through the TI of the group at the higher level to the TI of the group at the lower level group and finally to the targeted member at the lower level group and vice versa. The individual, group, and public keys are used (see, for example, column 4, lines 33-36) to encrypt and decrypt the data when data is stored in a data storage, transferred to a another storage within group, or transferred to a storage in a different group. Also, the TI at a higher-level group changes the group key for the TI at a lower level group (see, for example, column 4, lines 5-25, and column 13, lines 48-55). Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to add the hierarchical scheme of Mittra to the Boebert's system because it would provide a scalable electronic data storage

apparatuses system that would make the group more manageable and to transmit data and encryption keys among the groups and the electronic data storages with a higher security and efficiency (column 5, lines 39-56).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Pat. No. 6,292,899 to McBride

U.S. Pat. No. 5,915,025 to Taguchi et al.

U.S. Pat. No. 5,144,655 to Takaragi et a.

U.S. Pat. No. 5,784,464 to Akiyama et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 703-305-8074. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

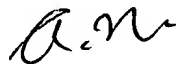
Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Abdulhakim Nobahar

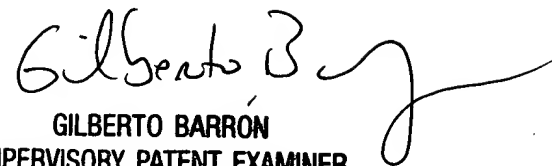
Application/Control Number: 09/327,477
Art Unit: 2132

Page 8

Examiner
Art Unit 2132



AN



GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100